Remarks

Reconsideration of the issues raised in the Office Action dated January 21, 2009 is respectfully requested in light of the amendments to the specification and the claims, and the remarks presented herewith. The issues are addressed below in the order in which they are presented in the Office Action.

Title

The title has been objected to as being "not descriptive."

In the amendments to the Specification presented herewith, a new title is presented that is indicative of the invention to which the claims are directed.

Specification

The abstract of the disclosure has been objected to as containing trademarks which have not been identified properly.

In the amendments to the Specification presented herewith, the abstract of the disclosure has been amended to more properly identify the trademark used therein.

The disclosure has also been objected to as lacking section headings.

In the amendments to the Specification presented herewith, the disclosure has been amended to include proper section headings.

Additionally, the use of the trademark WINDOWS in the application has been identified as requiring correction, and the examiner has encouraged the applicants to carefully check the Specification to ensure that no other trademarks have been used without proper capitalization and accompaniment by generic terminology.

In the amendments to the Specification presented herewith, the Specification has been amended to capitalize all known trademarks and to use generic terminology therewith.

It is respectfully submitted that amendments to the Specification adequately address the identified objections to the Specification, and it is respectfully requested that the stated objections be withdrawn.

Claim Objections

The objections raised with respect to claims 13 and 22 have been addressed in the amendments to the Claims presented herewith. Additionally, a misspelling has also been corrected in claims 17 and 19, and reference numbers have been removed from claims 9 and 10.

It is respectfully submitted that amendments to the Claims properly address the identified objections to the claims, and it is respectfully requested that the objections be withdrawn.

Claim Rejections – 35 U.S.C. 102

Claims 1 – 6, 9, 11 – 16, 20 – 24, and 26 have been rejected under 35 U.S.C. 102(b) as being anticipated by Ohashi et al. (U.S. Patent No. 5,761,309) ("Ohashi"). These rejections are respectfully traversed.

Claim 1 recites a method for carrying out an authentication process for authenticating a subsequent transaction by any one of a plurality of users with data processing apparatus, including, inter alia, the step during the authentication process of operatively associating with the data processing apparatus a selected one of a plurality of authentication storage means respective to the users, each authentication storage means storing predetermined authentication information, the predetermined authentication information stored by each authentication storage means corresponding to information which is used to authenticate that user's telecommunications terminal in relation to the telecommunications system (emphasis added).

It is alleged in the Office Action that "Ohashi disclosed a method for carrying out an authentication process for authenticating a subsequent transaction by anyone of a plurality of users with data processing apparatus (client) (Ohashi Abstract), including the step during the authentication process of operatively associating with the data processing apparatus a selected one of a plurality of authentication storage means (smart card) respective to the users, each authentication storage means storing predetermined authentication information ... (Ohashi Col. 12 Lines 19-29), ... the predetermined authentication information stored by each authentication storage means corresponding to information which is used to authenticate that user's telecommunications terminal in relation to the telecommunications system (Ohashi Col. 12 Lines 30-36)." This contention is respectfully traversed.

Ohashi discloses an authentication system whereby authentication load can be distributed in the network without sharing secret information of users (abstract). The passages of Ohashi cited above describe an authentication process carried out in a "two phase sequence" (col. 12, lines 15 – 18), the first phase being "request and issuance of a certificate" (col. 12, lines 19 – 29) and the second phase being "request and enjoyment of a network service" (i.e., obtaining permission information)(col. 12, lines 30 – 36).

Absent in Ohashi is any teaching that either of the two main steps (obtaining certificate or subsequently obtaining permission information) uses authentication information "corresponding to information which is used to authenticate that user's telecommunications terminal in relation to the telecommunications system," as recited in claim 1. If the certificate obtaining step (or a combination of both steps together) is treated as analogous to the "authentication process" of claim 1, the only available analogue for the "predetermined authentication information" in Ohashi is the "secret key Ku" stored in a memory of the smart card (read as the "authentication storage means) (col. 11, lines 51 – 54; col. 12, line 55 – col. 13, line 5). This is the only information Ohashi mentions as being stored by the smart card (information storage means), as required in claim 1.

However, the closest to a disclosure of any mechanism for connecting the client terminal of Ohashi to a "telecommunications network" is a passage on col. 5, lines 5 to 17. This passage only mentions "a network 13 such as for example a LAN." However, Ohashi does not contain a teaching or suggestion that the "secret key" is information used to "authenticate that user's telecommunications terminal in relation to the telecommunications system."

Claim 1 further recites that "the authentication process for authenticating the transaction by that user with the data processing apparatus" neither requires "use of that user's telecommunications terminal" nor requires "the telecommunications terminal to be actually authenticated by that information in relation to the telecommunications systems." The present invention makes use of the predetermined authentication information on the authentication storage means and uses this for authenticating a transaction with data processing apparatus where no telecommunications terminal is involved. In an embodiment described in the application, the user's SIM (authentication storage means) performs authentication with a remote service provider using the predetermined authentication information without involvement of the user's telecommunications terminal.

It is stated in the Office Action that Ohashi discloses "the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of that user's telecommunications terminal nor requiring the telecommunications terminal to be actually authenticated by that information in relation to the telecommunications systems (Ohashi Col. 5 Paragraph 2)." This contention is also respectfully traversed.

The second paragraph in column 5 of Ohashi describes a smart card 10, a client terminal 12, and describes that a network 13 may have a plurality of client terminals. It is respectfully submitted that neither in the second paragraph in column 5 nor elsewhere does Ohashi contain a teaching or suggestion of an authentication process using information which is used to authenticate the user's telecommunications terminal to the telecommunication system, but the authentication process not requiring use of that user's telecommunication terminal nor requiring the telecommunications terminal to be actually authenticated by that information to the telecommunications system, as recited in claim 1. It is respectfully submitted that there is simply no teaching or suggestion of a telecommunications terminal for which the "secret key" would be used to authenticate that terminal in relation to a telecommunications network in Ohashi.

Still further, claim 1 also recites, "each authentication storage means storing predetermined authentication information and <u>being registerable with a common telecommunications system for which the users have respective telecommunications terminals</u>."

MPEP 2111 requires that, during patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification" (emphasis added).

The term “registerable,” interpreted in the light of the specification as a whole and the illustrated examples in particular, certainly encompasses the registration of a SIM card with a cellular telecommunications network (via a suitable cellular terminal).

It is alleged in the Office Action that Ohashi discloses “each authentication storage means ... being registerable with a common telecommunications system for which the users have respective telecommunications terminals (Ohashi Col. 12 Lines 19-29).”

The cited passage of Ohashi describes the “request and issuance of a user certificate” phase of an authentication process, wherein the user (smart card 10) requests an authentication center 17 to issue a user certificate which verifies him.

It is respectfully submitted that this passage of Ohashi is not a teaching or suggestion of a “smart card” being registerable with a telecommunications system at all. In fact, the Ohashi reference does not contain a teaching or suggestion that the smartcards (i.e. authentication storage means) described therein are “registerable with telecommunications systems,” as recited in claim 1. It is noted that GSM is mentioned in Ohashi, briefly, in the “Background Art” section (col. 2, lines 35 – 43), but this brief mention not in relation to the smartcards being registerable with telecommunication system, (i.e., SIMs).

More specifically, neither of the two main steps in Ohashi – obtaining certificates or obtaining permission information – requires the use of a smartcard that is registerable with telecommunications systems. If anything, adding such a requirement would appear to be contrary to the general teaching of Ohashi which emphasises the need to minimise the dispersion of users’ secret information.

Accordingly, for the reasons described above, reconsideration and withdrawal of the rejection of claim 1 under 35 U.S.C. 102(b) is respectfully requested.

Independent claims 13 and 22 recite the same subject matter as discussed above with respect to claim 1, and are therefore allowable over Ohashi for at least the reasons provided in support of the allowability of claim 1.

Still further, dependent claims 2 – 6, 9, 11 – 12, 14 – 16, 20 – 21, 23 – 24, and 26 depend from one of independent claims 1, 13 or 22, and are allowable over Ohashi for at least the reasons provide in support of the allowability of the independent claims from which the depend, respectively.

Claim Rejections – 35 U.S.C. 103

Claims 7 – 8, 10, 17 – 19, and 25 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Ohashi. These rejections are respectfully traversed.

Claims 7 – 8 and 10 depend from independent claim 1, claims 17 – 19 depend from independent claim 13, and claim 25 depends from independent claim 22. It is respectfully submitted that claims 7 – 8, 10, 17 – 19, and 25 are allowable over Ohashi, alone, for at least the reasons provided above in support of the allowability of independent claims 1, 13, and 11 over Ohashi.

Furthermore, Ohashi gives no hint or pointer that might lead the skilled reader to adopt one type of authentication storage means over any other. Indeed, the focus in Ohashi is upon minimizing the dispersion of users' secret information (abstract). By contrast the present invention proposes "reusing" a smartcard (which could in principal be used in a telecommunications terminal to authenticate the establishment of a communications link via a common telecommunications system) – and consequently actually expands the distribution of users' secret information.

The present application pre-dates any published proposal of which the Applicant is aware where the SIM/authentication storage means is used separately from the telecommunications terminal. That is, the predetermined authentication information on the SIM, corresponding to information that is used to authenticate a telecommunications terminal with a common telecommunications network, is used to authenticate a transaction with a data processing apparatus by operatively associating the authentication storage means/SIM with the data processing apparatus, without the user's telecommunications terminal.

At the priority date of the present application there was a prejudice in the mobile telecommunications art against using an authentication storage means/SIM separately from a telecommunications terminal. Such a use of a SIM was never envisaged prior to the present application. The present invention provides a significant technical advantage of providing secure authentication, for example using the challenge and response SIM authentication between the SIM and the authenticating means of the common telecommunications system, to authenticate a transaction using a data processing apparatus with which the authentication storage means/SIM is operatively coupled. The authentication requires processing of the challenge and response to be performed at both ends of the communication channel over which the transaction is authenticated. The present invention enables secure and reliable authentication of transactions to be performed without developing new authentication infrastructure.

Given the significant technical advantages of the present invention, in the absence of any prior art disclosing or suggesting the claimed authentication arrangement, it is respectfully submitted that no rational reason has been provided in the Office Action which indicates that a person skilled in the art *would* modify any prior art document or "telecommunication authentication standards" in order to arrive at the invention as recited in independent claims 1, 13, and 22, and that the observations regarding the aspects of the dependent claims that were “known in the art” do not address the deficiencies of the Ohashi reference with respect to the independent claims.

As a result, it is respectfully submitted that the present invention (as set out in main claims 1, 13 and 22, and the claims that depend therefrom) is clearly non-obvious over the prior art.

Still further, to the extent that Official Notice is being taken in the rejections of claims 7 – 8, 10, 17 – 19, and 25, such finding is respectfully traversed. Claims 7 – 8, and 17 – 18 relate to levying a charge for a transaction when authenticated, and claims 10, 19, and 25 relate to the authentication storage means communicating wirelessly to authenticate the transaction.

With respect to levying a charge for a transaction when authenticated (claims 7 – 8, and 17 – 18), it is respectfully submitted that Ohashi relates confirming that a user is a "legitimate user" and not to levying a charge for a transaction when authenticated (see: specification, paragraphs [0042], [0053], [0056], [0085], [0146], [0151]-[0152], [0155]-[0156]). It is further believed that other art relating to such authentication processes at the time of the invention related to confirming that a user was a "legitimate user" and not levying a charge for a transaction when authenticated. Documentary evidence is respectfully requested if this rejection is maintained.

Further, while the use of SIMs for wireless communication may be common, it is respectfully submitted that "wherein the authentication storage means communicates wirelessly to authenticate the transaction" (claims 10, 19, and 25, see: specification, paragraphs [0045], [0087]-[0088], [0091], [0095], [0157]-[0158]) is not believed to have been well know at the time of the invention. Documentary evidence is also respectfully requested if this rejection is maintained.

Double Patenting

Claims 1 – 26 have been provisionally rejected on the ground of nonstatutory obviousness-type double patenting over claims 1 – 53 of co-pending Application No. 10/531,430 ("the '430 application") and all pending claims of co-pending Application No. 10/574,808 ("the '808 application").

A single terminal disclaimer based on common ownership, pursuant to MPEP 804.02.IV, is submitted herewith disclaiming the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration dates of the '430 application and the '808 application. It is respectfully submitted that the terminal disclaimer overcomes the provisional nonstatutory obviousness-type double patenting rejections.

Allowance of the application in its present form is respectfully solicited.

Respectfully submitted,

Date: July 21, 2009

/jeffrey a. haeberlin, reg. no. 40,630/

Signed By Name: Jeffrey A. Haeberlin
Attorney of Record Registration No.: 40,630

STITES & HARBISON PLLC ◆ 1199 North Fairfax St. ◆ Suite 900 ◆ Alexandria, VA 22314
TEL: 703-739-4900 ◆ FAX: 703-739-9577 ◆ CUSTOMER NO. 881

STATEMENT - SUBSTITUTE SPECIFICATION		
	Application #	10/531,429
	Confirmation #	8445
	Filing Date	10/24/2005
	First Inventor	LINCOLN
	Art Unit	2431
	Examiner	Henning, Matthew T.
	Docket #	P08620US02/BAS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

S I R:

In response to the Office Action dated January 21, 2009, Applicant is submitting herewith a substitute specification and abstract. In accordance with MPEP 608.01(q), Applicants submit herewith a clean copy of the substitute specification and abstract and a marked up copy of the substitute specification and abstract showing the changes from the originally filed specification and Abstract.

Applicant hereby states that the substitute specification and abstract include no new matter; as is readily evident from the marked up copy.

Respectfully submitted,

Date: July 21, 2009

/jeffrey a. haeberlin, reg. no. 40,630/
By: Jeffrey A. Haeberlin
Reg. No.: 40630